

Title (en)

IC CARD FOR SECURITY ATTESTATION AND IC CARD SERVICE SYSTEM USING SAID IC CARD.

Title (de)

IC-KARTE FÜR SICHERHEITSBESCHEINIGUNG UND IC-KARTENDIENSTSYSTEM, DAS DIESE VERWENDET.

Title (fr)

CARTE A CIRCUITS INTEGRES SERVANT D'ATTESTATION DE SECURITE ET SYSTEME DE SERVICE A CARTE IC L'UTILISANT.

Publication

**EP 0440800 A1 19910814 (EN)**

Application

**EP 90908656 A 19900605**

Priority

JP 14108689 A 19890605

Abstract (en)

A program for generating individual keys from a base key is stored in a memory in each SA card (12) in the production of SA cards. Next, the base key is stored in a secret area in the memory, data stored in which cannot be read out from outside, in the SA card (12) by an SA card issuing machine. When issuing individual user cards (13), a user card issuing machine transmits ID or the like of the card to the SA card (12), prepares the individual keys by use of the individual key generation program and stores the received individual keys in the secret area in the memory of the user card (13). At the time of use, the card ID or the like of the user card is transmitted from the user card (13) to the SA card (12) and the SA card prepares the individual key of the user card from the reception information and shares the individual key. In this manner, the IC card service system can execute various attestations by use of the functions such as encoding and decoding of data without making on-line inquiry to the center side.

Abstract (fr)

On enregistre un programme générateur de clés individuelles à partir d'une clé de base dans la mémoire de chacune des cartes SA (12) lors de leur fabrication. On enregistre ensuite la clé de base dans une zone secrète de la mémoire, empêchant la lecture depuis l'extérieur des données qu'elle contient, dans la carte SA (12) à l'aide d'une machine d'émission de cartes SA. Lors de l'émission de cartes utilisateur individuelles (13), une machine d'émission de cartes utilisateur transmet l'ID ou similaire de la carte à la carte SA (12), prépare les clés individuelles grâce au programme générateur de clés individuelles et stocke les clés individuelles reçues dans la zone secrète de la mémoire de la carte utilisateur (13). Lors de l'utilisation, l'ID de la carte utilisateur est transmis de la carte utilisateur (13) à la carte SA (12) et cette dernière prépare la clé individuelle de la carte utilisateur à partir des informations de réception et partage la clé individuelle. Le système de service à carte IC peut ainsi exécuter différentes attestations, en utilisant des fonctions telles que le codage et le décodage de données sans effectuer des interrogations en ligne adressées à l'ordinateur central.

IPC 1-7

**B42D 15/10; G06K 17/00; G06K 19/00; G07F 7/08; G09C 1/14**

IPC 8 full level

**B42D 15/10** (2006.01); **G06F 12/14** (2006.01); **G06K 17/00** (2006.01); **G06K 19/07** (2006.01); **G06K 19/073** (2006.01); **G06K 19/10** (2006.01); **G07F 7/10** (2006.01)

CPC (source: EP)

**G06Q 20/229** (2020.05); **G06Q 20/341** (2013.01); **G06Q 20/3558** (2013.01); **G06Q 20/40975** (2013.01); **G07F 7/1008** (2013.01); **G07F 7/1016** (2013.01)

Cited by

DE19804054B4; FR2810139A1; EP0722596A4; US6128391A; FR2759833A1; US5923759A; US5381478A; EP0500245A3; US5406624A; EP0587375A3; FR2760871A1; FR2670036A1; US8316221B2; EP0707290A1; FR2725537A1; AU690324B2; US5825875A; EP0635774A3; EP1383073A4; US7602920B2; US7409554B2; US6658566B1; US6487660B1; WO9421878A1; WO9837525A1; WO9848389A3; WO9851032A3; WO9840853A1; WO9916031A3; WO0195274A1; WO9933033A3; US7822987B2; US8307211B2; US8966271B2; US9990796B2

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

**WO 9014962 A1 19901213**; EP 0440800 A1 19910814; EP 0440800 A4 19970924; FI 910537 A0 19910204; JP 2731945 B2 19980325; JP H037399 A 19910114

DOCDB simple family (application)

**JP 9000727 W 19900605**; EP 90908656 A 19900605; FI 910537 A 19910204; JP 14108689 A 19890605